Public Folders, Groups, and ACLs in Platinum

Updated: 20 January, 2000

Background

Exchange 5.5 Distribution Lists

In ExDS, a distribution list can have as members a mailbox from any site in the organization and/or another distribution list. This nesting of DLs is not limited, nor is there any special requirements with respect to the mailboxes – if it exists in the org, it can be a member. Exchange DLs are used for two functions in Exchange 5.5 – email distribution lists and for specifying ACLs on Public Folders.

Windows NT4 Groups

Although we do not use them extensively within Exchange 5.5, Windows NT4 supports two types of groups – both are only security related and do not incorporate any email functionality. Domain Local groups can have membership from any trusted domain, but the scope of the group is restricted to only the local domain. That is, it can only be used to ACL a resource that exists in the same domain as the group itself. Domain Local groups cannot be nested. The second type of group is Domain Global; these can have membership from only the local domain, but it has a global scope. Global groups can be referenced in ACLs on resources in any domain. Domain Global groups can have one level of nesting. There is no group type that corresponds to the membership and scope of an Exchange 5.5 DL.

Windows 2000 Groups Add Flexibility

Windows 2000 supports the Windows NT4 style group mentioned above, plus adds a new group type and the ability to associate an email address (mail-enable) with a group. The new group type is called Universal groups. Universal groups support the nesting and membership behavior that we have in Exchange 5.5 DLs – membership can be from any domain and the group can be referenced in any domain.

Security Groups vs Distribution Groups

In Windows 2000, all groups can have any of two properties: a group can be mail-enabled and / or it can be security-enabled. A group that is mail-enabled is termed a “distribution group”, a group that is security-enabled is a “security group”, and a group that is both is a “mail-enabled security group”. In certain

circumstances, a distribution group can be converted into a mail-enabled security group. In order for a group to be used to ACL a resource, it must be a security group.

Windows 2000 Domain Modes and Group Restrictions

Windows 2000 domains can operate in either “mixed” or “native” mode. In mixed mode, the domain may contain NT4 domain controllers and it is therefore restricted to supporting only the group types that Windows NT4 supports. Specifically, this means that mixed mode domains cannot support Universal security groups. Universal Security Groups are only supported in native mode Windows 2000 domains. A native mode Windows 2000 domain only contains Windows 2000 domain controllers and the “native mode” setting has been enabled.

Active Directory Connector and DLs

The Active Directory Connector will replicate all Exchange 5.5 DLs to the Active Directory as Universal Distribution Groups. This group type was selected because the majority of DLs in 5.5 are only used as distribution lists, not in ACLs. Also, the Windows 2000 team is recommending that customers use Universal Security Groups cautiously since their over-use can lead to “token-bloat”. So, this means that immediately after ADC replicates the 5.5 DLs to AD they can be used as email distribution groups, but not for assigning permissions in ACLs.

The Problem

Since 5.5 public folders have ACLs and we can replicate PFs to Platinum (or upgrade a 5.5 PF to Platinum), then we need a means of representing that ACL. In the case of folders ACLd with a DL, we cannot simply use the Universal Distribution Group that the ADC created because it is not a security group. We cannot have all of the DLs be created as security groups because of the token bloat concern and because many of the users will be in mixed mode domains and their logon-generated token will not include the SIDs of the USGs. So, we need to do some special handling of the group and the token.

Key Aspects of the Solution

USGs with mixed mode membership

Windows 2000 has done work in RTM to support a USG that has member objects that exist in mixed mode domains (the USG itself must still be in a native mode domain). When a user logs on to a mixed mode Windows 2000 domain, a token is

constructed that contains the user object's SID and the SIDs of any global groups of which it is a member. USG membership is only evaluated at logon and included in the token when the user object exists in a native mode Windows 200 domain.

Token augmentation

Given that we need to support the interoperation of Exchange 5.5 and Platinum, we had to devise a mechanism by which to extend the token of the mixed mode Windows 2000 user to include the SIDs of the USGs of which it is a member. The NT team provided functions to facilitate this token augmentation, and it is being incorporated into the code path in DAV, OLEDB, MAPI, and IFS. So, the logic we have developed will augment the token as necessary, taking into account whether the user is in a native or mixed mode Windows 2000 domain and if a disabled user object is involved (see *added complexity…* below).

Converting UDGs to USGs

Not all Exchange DLs are used for setting permissions on public folders, only a subset. One of the downsides to Universal Security Groups when in native mode Windows 2000 is that their overuse can lead to "token bloat". That is, if all distribution lists were blindly converted to USGs, then once users are in native a native mode domain they would end up with huge tokens (and slower login response). So, we need to be selective about converting UDGs to USGs, and only convert those that are being used to permission public folders. The conversion process will need to occur at three points: during upgrade from 5.5, during public folder replication with 5.5, and whenever a user defines permissions on a Platinum public folder and specifies a distribution group. The store will need to log events as to the cusses or failure of these conversions and also take into account the nested nature of distribution groups.

Disconnecting user domain upgrades from Platinum deployment

A primary design goal for the solution was to enable customers to proceed with Platinum deployment in advance of full conversion to Windows 2000 native mode across their domains. While USGs do require a native mode domain, the approach we are taking allows customers to deploy a dedicated native mode "group management domain" that is used as the target of an ADC connection agreement for distribution lists. Since it is native mode, the UDGs can be successfully converted into USGs as necessary, without impacting the customer's user authentication domains. Once they have upgraded their user domains to native mode, the groups can be moved into that domain(s) and the group management domain can be removed from the topology.

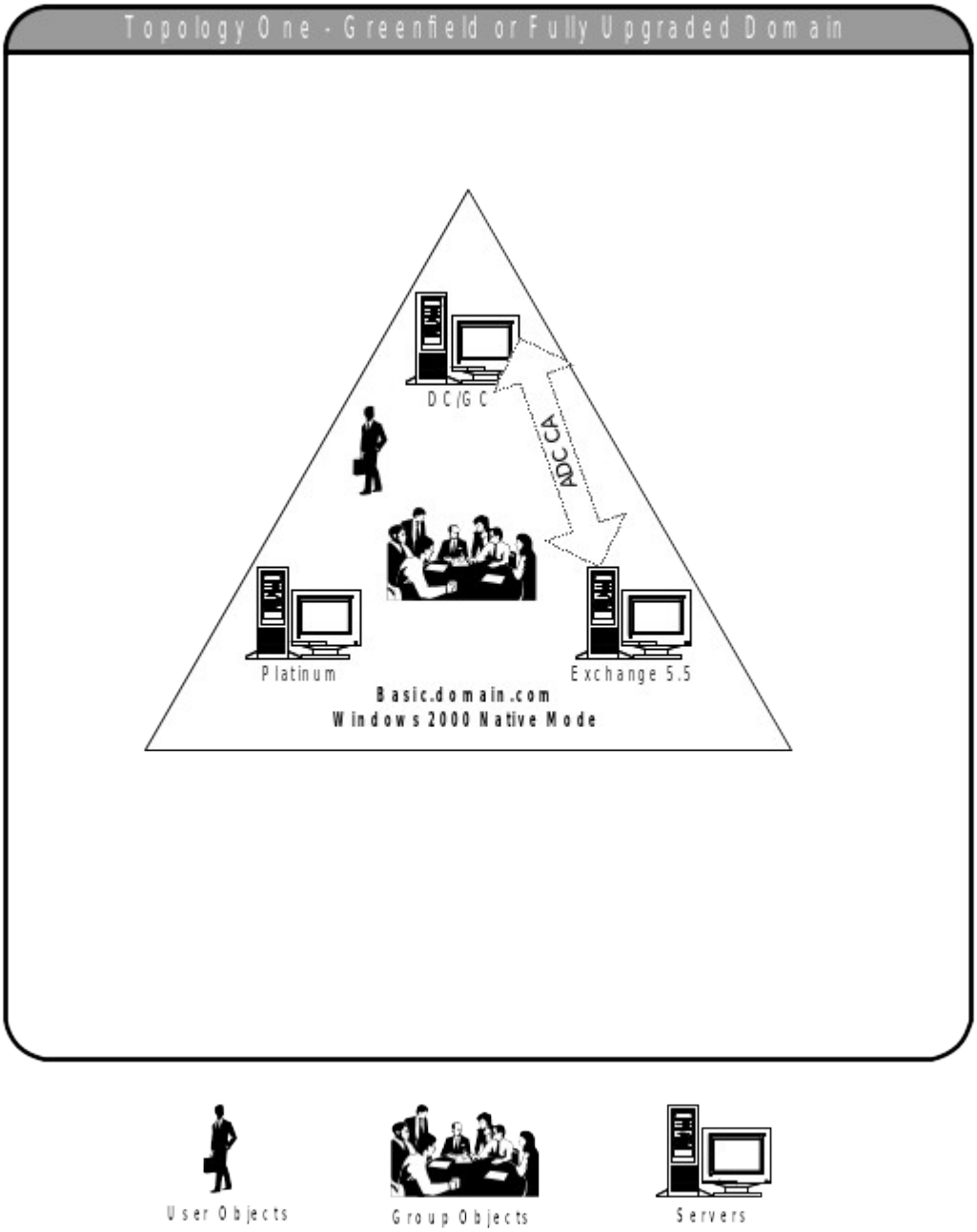
Added complexity from disabled users and mailbox rights

In some customer deployments (and in dogfood) there will be instances where the Platinum mailbox is actually a disabled user object and mailbox rights have been assigned to a user object (or NT4 account) in a trusted domain. This complicates the token augmentation logic in that it now needs to check for the presence of Exchange Master Account SID and acquire the corresponding disabled user object. It is this disabled user object that will be a member of USGs, not the trusted account. So, once the object is acquired, the augmentation logic can continue, adding the SIDs of the USGs of which this disabled user is a member to the token. Additionally, when disabled users are used and the mailbox rights are assigned to a user in a native mode domain, the msExchAddGroupsToToken attribute must be set to force the token augmentation logic to be invoked.

Five Test Topologies

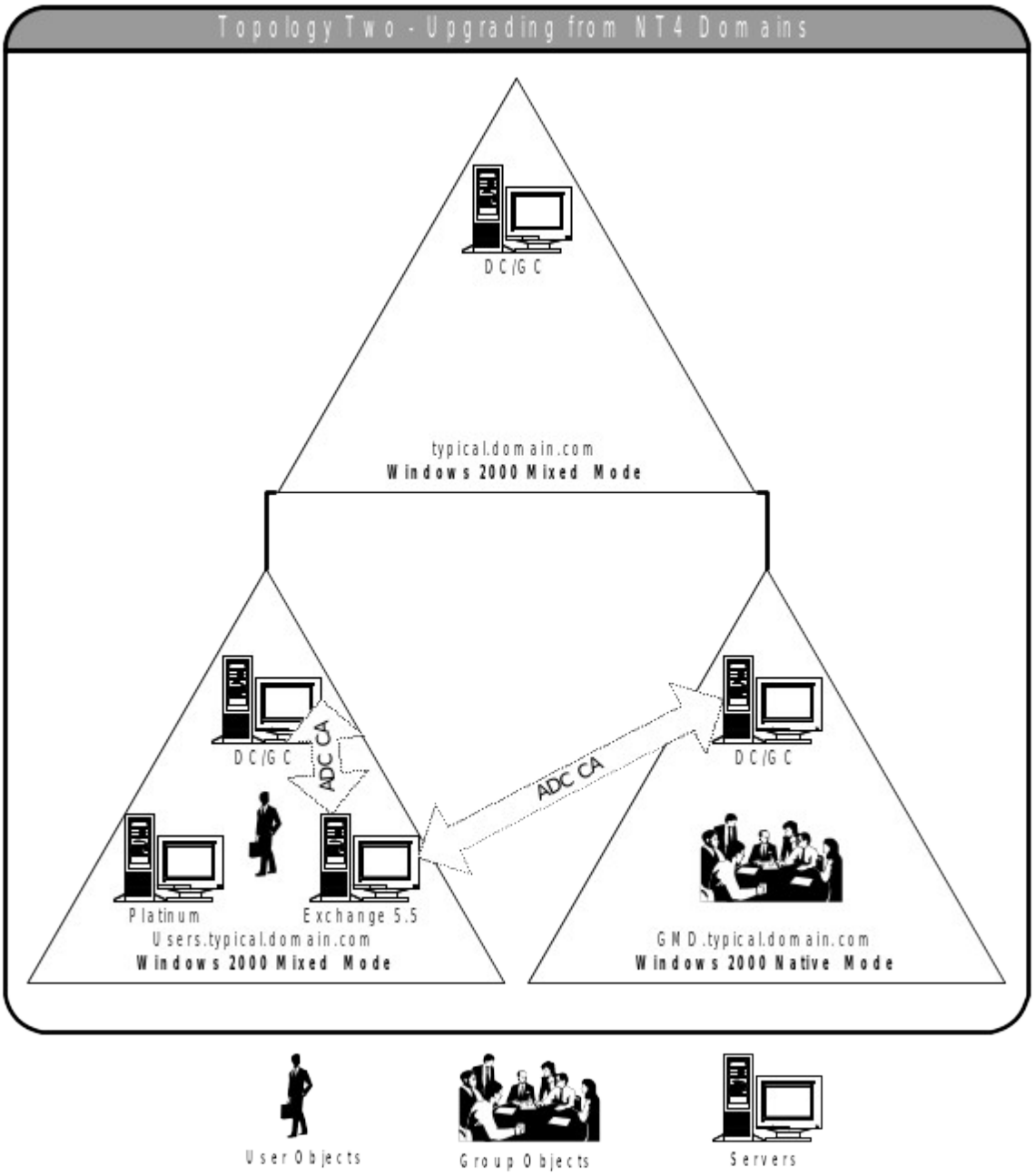
The Universal Security Group / Public Folder ACL testing falls into five basic topologies. Each topology is depicted below with a brief explanation of its differentiating elements. The diagrams are minimum installations – additional testing with more "real-life" environments (multiple Windows 2000 sites, multiple DCs, multiple GCs, multiple domains) should be done prior to production deployment to verify that nothing breaks with added complexity.

1. **Single Native Mode Domain** – This is the simplest case; all user and group objects are in a native mode domain. The Store is therefore able to convert the universal distribution groups into universal security groups and at ACL evaluation time we do not need to invoke the token augmentation logic path (since the user's token will already include the USGs). A variation on this would be a forest of multiple native mode domains.



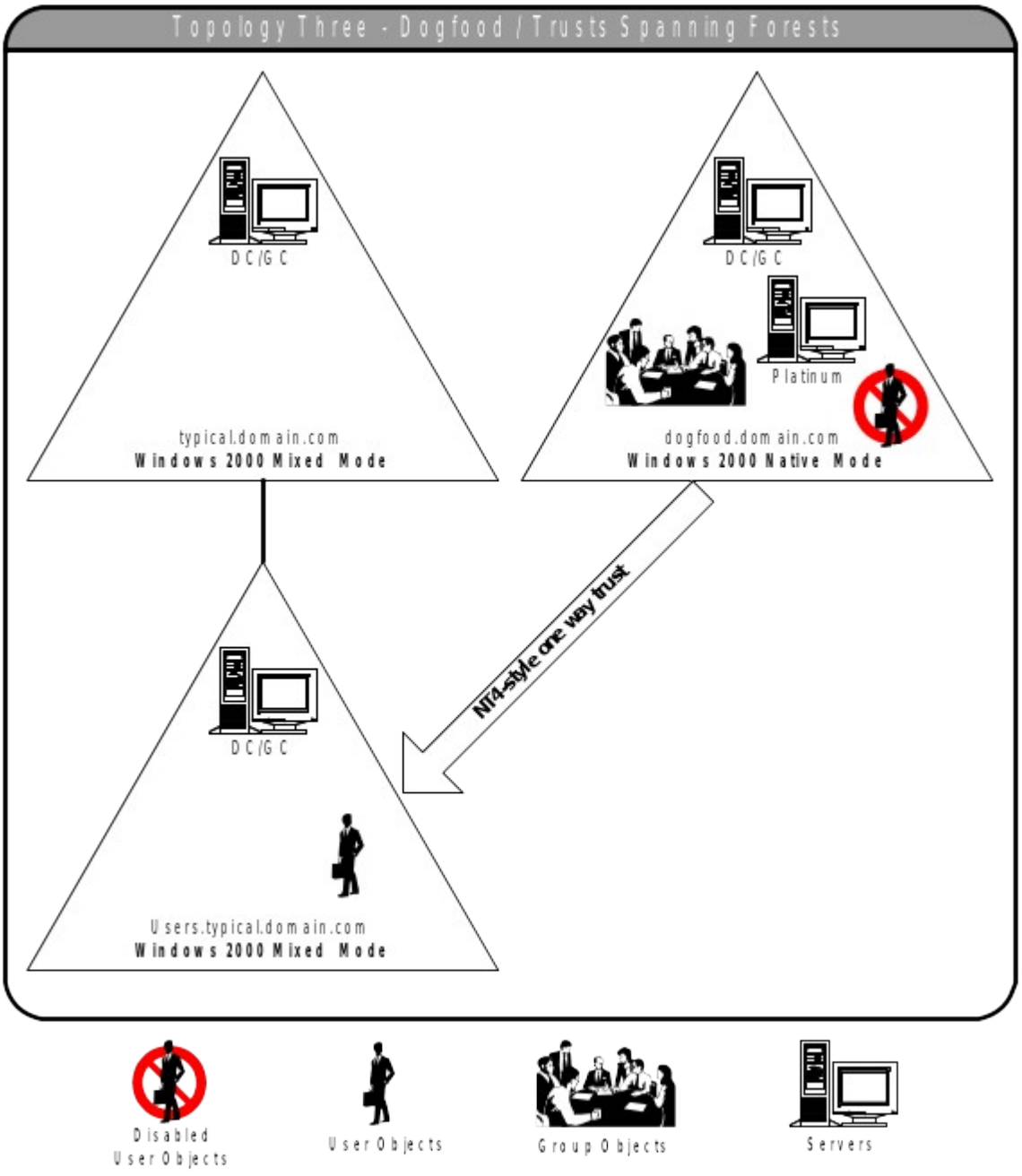
2. **Group Management Domain** – This is expected to be the majority case for customers upgrading from Exchange 5.5 as well as for many new customers. The user objects and the Platinum servers may be in mixed mode Windows 2000 domains. This needs to be supported in order to provide customers a path to Platinum that does not require waiting until they have fully deployed Windows 2000 and enabled native mode on all of their domains. In order to have universal security groups, we must have at least one native mode “group management” domain in the topology that will be used to host groups. The token augmentation logic will be used to add the SIDs of the USGs of which the user object is a member

into the token prior to evaluation.

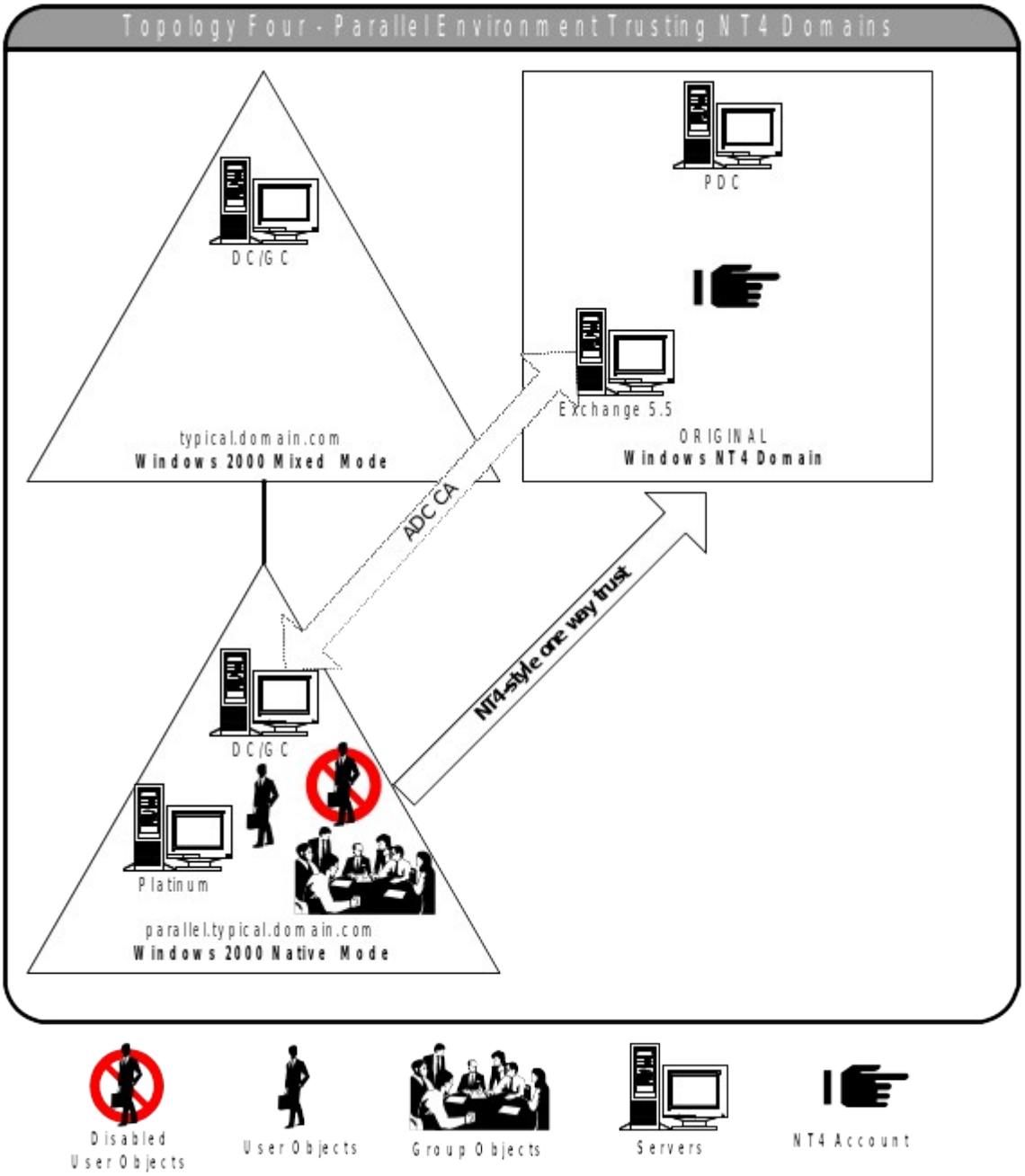


3. **Dogfood** – The important case for this topology is that we have a situation where the user is logging on with credentials from an explicitly trusted domain and accessing a Platinum server in a different forest. So, you end up with a Platinum disabled user object that has mailbox rights assigned to an enabled user object in the trusted authentication domain. This added level of complexity is dealt with via the Exchange Master Account SID attribute. The token augmentation code determines that we are in this situation, finds the corresponding disabled user object, and augments the token with the SIDs of the universal security groups of which that

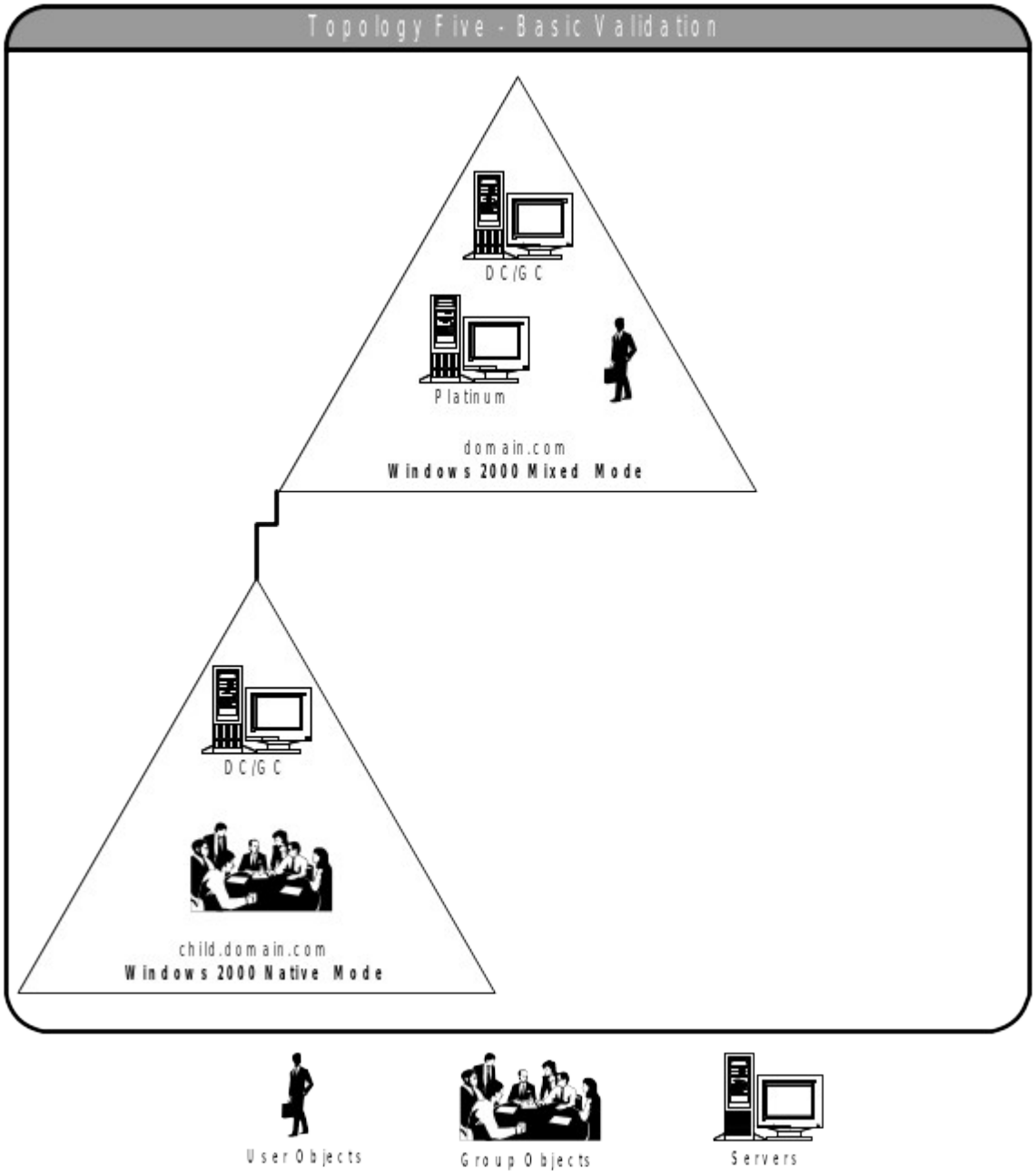
object is a member.



4. **Windows 2000 Domains Trusting NT4 Domains –** This will be an important case for customers whose NT4 domain architecture is bad enough to warrant not upgrading it. These customers will instead deploy a pristine Windows 2000 environment in parallel, trusting the original NT4 domains. This results in a situation where a disabled user object in the domain with Platinum has mailbox rights assigned to an NT4 account in the trusted authentication domain. As in Topology Three, the added level of complexity is dealt with via the Exchange Master Account SID attribute and the augmentation logic takes this into account.



5. Basic Token Augmentation Validation - The token augmentation code path can be verified by taking all of the other variables involved with the previous scenarios out of the topology. So, the basics you are left with are: Platinum and user objects in a mixed mode domain, and a child native mode domain. Create a universal security group in the child domain and add as a member a user from the mixed mode domain. Create a public folder in Platinum and assign permissions to the universal security group. Access the public folder from the user that you created. The expected behavior is that token augmentation will have added the SID of the USG in the user's token, thus enabling access to be successful. This removes the questions of PtOz, PF replication, and group conversion from the equation, leaving only the token work.


Topology Five - Basic Validation
DC/GC
Platinum
domain.com
Windows 2000 Mixed Mode
DC/GC
child.domain.com
Windows 2000 Native Mode
User Objects
Group Objects
Servers